ManTech
Security & Mission Assurance

MANTECH SMA
COMPUTER FORENSICS & INTRUSION ANALYSIS

VULNERABILITY ASSESSMENT & PENETRATION TESTING EXECUTIVE SUMMARY REPORT

STATE AUDITOR, STATE OF NORTH DAKOTA

This report and included attachments contain data specific to the State of North Dakota's computer network. The disclosure of information contained in this document could impact the function of the State of North Dakota's computer network, and possibly allow its security controls to be bypassed. The information contained in this document must be protected from disclosure to unauthorized individuals. This document should only be shared with persons directly involved in the limited security assessment requested by the State Auditor or persons authorized by the State Auditor. This assessment is a snapshot in time and any new vulnerabilities introduced after the completion of this assessment will not be identified here.

ManTech Security & Mission Assurance, a group of ManTech International Corporation

PH (703) 847-6070 • www.mantech.com • FAX (703) 847-5787

Leading the Convergence of National Security and Technology

DOCUMENT VERSION HISTORY

Version	Date	Author	Change Description
1.0	23 October 2007	Mark Shaw	Initial Report
1.1	26 October 2007	Mark Shaw	Minor Edits
2.0	2 November 2007	Mark Shaw	Final Draft

TABLE OF CONTENTS

November 6, 2007

The Honorable John Hoeven, Governor
Members of the North Dakota Legislative Assembly
Lisa Feldner, Chief Information Officer, Information Technology Department

Transmitted herewith is the security audit of the state network. This audit resulted from the statutory responsibility of the State Auditor under NDCC § 54-10-29.

The Office of the State Auditor contracted with ManTech Security & Mission Assurance to perform this audit.

Inquiries or comments relating to this audit may be directed to Donald LaFleur, Information Systems Audit Manager, by calling (701) 328-4744. We wish to express our appreciation to the Information Technology Department and ManTech Security & Mission Assurance for the courtesy, cooperation, and assistance provided during this audit.

Respectfully submitted,

Robert R. Peterson
State Auditor

1. INTRODUCTION

No organization is immune to network intrusions. In this age of increased communication, the rate of electronic activity has grown exponentially as consumers and organizations find more opportunities to engage in transactions that involve the use of both the Internet and corporate networks. As a result, large organizations have become targets of individuals and groups seeking to gain "unauthorized access" for which they are unprepared and vulnerable. Not only are organizational network security breaches increasing in number and scope, they are causing more damage than ever before. Millions of dollars are lost each year and proprietary data and personally identifiable information is stolen as a result of network intrusions.

Vulnerability Assessments and Penetration Testing give organizations an opportunity to thoroughly and realistically evaluate the security posture of their IT infrastructure. This type of testing also allows the organization to assign relative risks to all vulnerabilities that are discovered. This allows for a quantitative risk analysis of vulnerabilities, and provides a basis for prioritization of fixes and countermeasures. Combining the technical vulnerability information with the organization's overall threat environment and risk tolerance, results in a clear risk picture that can be used to create a comprehensive mitigation plan.

During the period of August-September 2007, the Computer Forensics and Intrusion Analysis (CFIA) Group of ManTech Security and Mission Assurance (SMA) performed a Vulnerability Assessment and Penetration Test for the State Auditor of the State of North Dakota. This assessment consisted of four phases. The first phase was an External Vulnerability Assessment intended to provide the State a snapshot of the overall security and risk picture of the State's network from the Internet. The second phase was an Internal Vulnerability Assessment which assessed the State's internal network while emulating the insider threat as both a person with limited access and knowledge and also as the trusted – curious, malicious, or unwitting insider. The third phase consisted of a Penetration Test which sought to gain access to State systems from the Internet and test the State's security monitoring and response process. The final phase included an Application Security Assessment of the State's Peoplesoft Financials application. The Application Security Assessment gives the State an opportunity to thoroughly and realistically evaluate the security posture of this application and its associated components.

Vulnerabilities were assigned a risk identifier that was relative to the network or system under test. These identifiers were intended as a notional representation of the severity of the vulnerability. The three risk levels used are defined below:

High Risk – A high likelihood of compromise of system level access exists. If exploited this vulnerability may allow total control of the system.

Medium Risk – A vulnerability exists that may provide access to critical data and/or user level access to a system. This vulnerability may lead to further exploitation.

Low Risk – A vulnerability exists that may disclose information but does not directly lead to the exploitation of a system.

2. EXTERNAL VULNERABILITY ASSESSMENT

2.1 Overview

The Internet is an integral part of an organization's day-to-day business and operations. Due to its open nature, the Internet is also a tool that is often used by attackers to disrupt an organization's ability to perform normal business activities. Like most entities, the State of North Dakota has an information infrastructure that utilizes the Internet, making it vulnerable to Internet-based attacks. These attacks can lead to a loss of sensitive data, data integrity, productivity, time, and be costly to correct.

An External Vulnerability Assessment is intended to provide an organization a snapshot of the overall security and risk picture of the network from an external (Internet) point-of-view. External assessment procedures focus on performing Internet research, discovering systems connected to the Internet, and selectively probing these systems to discover misconfigurations and vulnerabilities.

During the period of August 13-22 2007, the Test Team performed an external vulnerability assessment of the State of North Dakota's statewide computer network. The assessment performed was a "limited knowledge" assessment in which the Test Team was only provided ranges of network addresses to assess.

2.2 External Vulnerability Assessment Approach

The assessment approach used for this phase of the assessment consisted of passive and active mapping followed by a complete vulnerability analysis.

2.2.1 Passive Mapping

This step emulated an outside threat (the average hacker) with limited knowledge of the network and involved enumerating the network and critical systems through open source techniques such as:

- Network and domain registrations
- Network administrator profiles (resumes, newsgroup postings, etc.)
- Web and news group postings
- Internet Research

This type of information gathering technique is frequently used by attackers to identify targets and obtain valuable information about a target. Passive mapping is an extremely effective data collection technique because the target is unaware intelligence is being collected.

2.2.2 Active Mapping

Once the passive mapping step was complete, active network probing began with small stealthy probes and escalated to the use of very "loud" commercial tools to identify

externally-facing systems on the State's networks. Enumeration tools were used to identify critical resources that touch the Internet. Methods in this step included the following:

- DNS Zone transfers
- Single packet probes to specific targets
- Operating system identification scans
- Identifying server loads through custom packet probes
- Service and application scanning
- "Bulk vulnerability" commercial scanning engines

2.2.3 Vulnerability Analysis

Once the various devices that were accessible from the Internet had been identified and information about those devices cataloged, the process of identifying potential vulnerabilities began. Once all information was correlated, the Test Team attempted to confirm that identified vulnerabilities were valid and did not represent false positives or were mitigated through other defenses.

2.3 External Vulnerability Assessment Results

2.3.1 General Recommendations

The following recommendations were provided to the State as a result of analysis performed on the data found during both the passive and active mapping stages of this assessment.

Review Content Available on Publicly Accessible Servers
A limited review of information available on State of North Dakota websites revealed a large amount of sensitive information that is publicly available. The Test Team was able to quickly locate State Information Technology standards, IT security services information, and robust search tools to collect contact information for State employees. It is recommended that the State fully review content available on all publicly accessible servers. Although some of this information may be required to be publicly available, websites that contain data only meant for internal State users should be restricted from being accessed from the Internet. The State must balance its requirements to provide information to the public with ensuring the security of it's networks.

Filter Inbound Access to All State Systems
Multiple systems were found to be running services that should be restricted from external access by IP-based access controls. Examples include databases (SQL, MYSQL, etc), printers, and Microsoft NETBIOS services. For the instances where external access to these services is required, IP-based access controls should be put in place to restrict

access to approved systems and services. It should be noted that the vast majority of systems without filtering in place resided on K12 and EDU networks.

Ensure Segregation Between K12/EDU and State Networks

Cursory review of the K12 and EDU networks reveal that they continue to be a weak link and the State should remain cautious in allowing these subnets access to State controlled networks. Due to the shared nature of the State's network, the security posture of each agency directly impacts the security of all the other agencies. Many systems were found to be directly connected to the Internet without any type of access restriction or control. Having default system services exposed to access by anyone greatly increases the risk to all systems on the network. For example, a worm outbreak within the systems of one agency could quickly propagate internally and consume bandwidth affecting the State's use and operation of its network.

2.3.2 Vulnerability Findings

Multiple tools were used to perform both automated and manual vulnerability scans against specific systems as requested by the State. Overall, 313 systems at State Agencies or organizations were found to have at least one vulnerability that would provide an external attacker with a possible attack vector that could lead to the compromise of the State's network from the Internet. Numerous other vulnerable systems were also found on K12 and EDU networks however a detailed analysis of these vulnerabilities was outside the scope of the assessment. For systems found on State controlled networks, there were 10 unique high risk vulnerabilities found on multiple systems, 2 unique medium risk vulnerabilities found on multiple systems, and 4 unique low risk vulnerabilities found on multiple systems. These vulnerabilities could generally be classified into three categories; architectural design flaws, misconfigured systems or applications, and operating systems or software applications that were missing critical security patches.

3. INTERNAL VULNERABILITY ASSESSMENT

3.1 Overview

An Internal Vulnerability Assessment is intended to provide an organization with a snapshot of the overall security and risk picture of the systems and network under assessment. Internal assessment procedures focus on examining networked systems for known vulnerabilities, misconfigurations, and implementation flaws that may expose the system to additional risk and is comprised mostly of automated testing complimented by manual inspection.

During the period of August 27 - September 5 2007, the Test Team performed an internal vulnerability assessment of the State of North Dakota's internal network.

3.2 Internal Vulnerability Assessment Approach

ManTech SMA began the internal assessment with a review of open ports, protocols, and shared resources on each system. This phase of the internal assessment emulated the insider threat as both a person with limited access and knowledge and also as the trusted – curious, malicious, or unwitting insider. Sources of these types of threats range from cleared cleaning crews, maintenance workers, temporary employees, and other individuals (who can gain some type of access to the facility and/or network but have no privileges on the system) to typical system users that use the network daily to fulfill their job duties.

After obtaining internal network access, the Test Team conducted a thorough vulnerability assessment, similar in nature, but much more comprehensive in scope than the external security assessment. The goal of the internal assessment was to identify potential vulnerabilities in the systems, as well as potential risks to critical data and systems, and recommend solutions to mitigate those risks. We tailored the assessment to each target set with the overall objective being to emulate the given threat as closely as possible to provide an accurate risk assessment of the system and the data it contains.

3.2 Internal Vulnerability Assessment Results

ManTech SMA performed a review of the State's network to access its overall security posture. This review included both manual and automated testing techniques.

3.3.1 General Recommendations

As a result of the review, the following recommendations were provided to the State to bring them in line with current security best-practices.

Segment Public Facing Servers from Internal Network

A main concern is the translation of public IP addresses to systems directly on the State's internal network. Compromise of one of these servers, which are publicly available, would allow an attacker direct access to the internal network. Once on this network, an

attacker would encounter limited restrictions to other internal systems. In accordance with security best practices, systems which are accessed from the Internet should be isolated in a DMZ configuration. This adds an additional layer of protection as the compromise of one of these systems does not provide immediate access to the internal network. Systems placed in the DMZ which require access to internal systems (e.g. authentication, backup, database connections, etc), should be strictly controlled by access-lists on an IP-to-IP and port-to-port basis. Also, systems located in the DMZ should be restricted from initiating outbound connections to the Internet unless explicitly allowed.

Internal Segregation of Critical Servers and Development Systems

Critical servers appear to be fully accessible from the internal network. It is recommended the State segregate servers deemed to be hosting critical data or services from the internal network by hosting these servers on a separate subnet strictly controlled by access-lists on an IP-to-IP and port-to-port basis. Lack of access control to these systems increases network exposure and risk from malicious users, worm and virus outbreaks. Additionally, development servers are currently hosted on the State's production network. Development systems are typically default, unpatched installs which can pose a serious security risk to the rest of the network. It is recommended development systems be completely isolated on a separate subnet with no access to other State resources (e.g. email).

Include Applications in Formal Patch Management Program

Multiple systems were found to be missing critical application security patches. It is recommended the State institute a formal, centrally-managed patch management program to require State agencies to regularly download and install application patches in addition to Operating System patches and establish a set maintenance period for each server to ensure that systems are rebooted on a regular schedule to complete the patch installation process.

Implement Outbound Access Control

There appear to be no outbound restrictions on traffic leaving the State's network destined for the Internet. Incidents, such as worm outbreaks, on the internal State network could affect external systems on the Internet. Additionally, malicious programs, such as spyware, or non-approved programs, such as peer-to-peer file sharing applications, could take advantage of this lack of outbound control to access the Internet. Security best practices utilize the principle of implicitly allowing certain types of traffic while denying everything else. The State should implement outbound access controls to allow only ports/services (HTTP, HTTPS, etc) approved by the State. The State should also implement outbound web filtering to actively enforce its Acceptable Use Policy. A user could place his system and the network at risk by visiting (intentionally or unintentionally) malicious websites without outbound filtering in place. This also reduces the ability for malware/spyware to make outbound connections.

Require use of Encrypted Protocols for Remote Management

Large numbers of systems on the State's internal network were noted using unencrypted protocols for remote access and management of systems. These protocols included the following:

FTP
Telnet
VNC
R-Services

Systems using unencrypted protocols are vulnerable to sniffing. Security best practices recommend the use of encrypted protocols for remote access and management. In some cases, these systems may not be capable of using encrypted protocols. However, it is recommended critical systems utilize only secure protocols and where possible implement IP-based access restrictions.

3.3.2 Vulnerability Findings

Multiple tools were used to perform both automated and manual vulnerability scans against specific systems as requested by the State. Overall, 427 systems were found to have at least one vulnerability that would provide an attacker with a possible attack vector that could lead to the compromise of the State's network and sensitive information. There were 29 unique high risk vulnerabilities found on multiple systems, 8 unique medium risk vulnerabilities found on multiple systems, and 4 unique low risk vulnerabilities found on multiple systems. These vulnerabilities could generally be classified into three categories; architectural design, misconfigured systems or applications, and the majority being operating systems or software applications that were missing critical security patches.

4. PENETRATION TESTING

4.1 Overview

A penetration test is intended to provide an organization a snapshot of the overall security and risk picture of its network from an external (Internet) point-of-view. Penetration testing focuses on gaining access to systems under an organization's control. Often a single system can provide a foothold into an organization's network and allow further access to external and/or internal systems. A penetration test requires extensive Internet research, identification of an organization's external systems and selectively probing these systems to discover misconfigurations and vulnerabilities. Additionally, penetration testing provides a means to capture the responsiveness of an organization's security devices and personnel.

During the period of September 5-10 2007, the Test Team conducted a penetration test of the State's network.

4.2 Penetration Testing Approach

Penetration testing seeks to gain unauthorized access to systems, passing data that should be rejected/dropped by the network security controls, or disrupting communications to or between systems. Access includes user or administrator level privileges on systems, the ability to read/write/modify/delete data on protected systems, or the ability to adversely affect system operation. Penetration testing is performed from external Internet access points. For the purposes of this test, a specific threat was be emulated; a malicious outsider with only access to information that can be recovered from the Internet. It is important to note that during penetration testing, exploit and privilege escalation tools and techniques were run by test team personnel, but no physically destructive attacks were performed.

The objectives of the network penetration test were to ascertain:

1. If security controls are properly implemented and functioning
2. Attack vectors that can cause harm to systems
3. The means to use said attack vectors to gain access to systems and data
4. Unauthorized use of technologies within that can put systems at risk
5. Security training and compliance with security policies
6. Personnel activities in response to threats and intrusions

This penetration test has three goals:

1. To emulate a realistic technical threat to the State computer networks from persons having no prior access or knowledge other than information that is openly available on the Internet.
2. To discover and exploit any vulnerability or combination of vulnerabilities found on the system in order to meet the stated objective of the penetration test.
3. To test the extent an organization's security incident response capability is alerted and to gauge the response to such suspicious activity.

Vulnerabilities can include unpatched services, misconfigurations, and poor security practices. Exploiting a vulnerability is dependent on several factors:

- **Impact** – Some exploits can cause services to crash. ManTech SMA tested all exploits within the safety of a closed test bed in order to minimize impact to State systems. Exploits that have the potential of causing long-term impact to the State's business proceses were not used against production systems.
- **Availability** – Due to time constraints, the Test Team leveraged existing public exploits (with modifications as needed), but the lack of a public exploit does not mitigate the risk of a particular vulnerability.
- **Time** – Many vulnerabilities can be time dependent. A good example would be password cracking. Generally any password can be broken given enough time and computing power. The Test Team had a set time frame for the penetration test, but an attacker would not be hindered by time constraints or test controls.

In addition to directly attacking State systems connected to the Internet, the Test Team used various social engineering techniques to target users of the State's internal network. Social engineering is part of penetration testing and involves the attempt to gain information or access through means other than through technical vulnerabilities. However, in some cases social engineering leverages technical vulnerabilities and weaknesses. The social engineer uses a combination of knowledge, salesmanship, and trickery to get members of an organization to break security policy by revealing passwords, customer data, or other privileged information.

Social engineering attacks commonly use the telephone or Internet to trick people into revealing sensitive information, or get them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that "users are the weak link" in security and this principle is what makes social engineering possible. The information gathered in this phase usually falls into the following two categories:

- E-Mail and Web-Based Exploitation
- Telephonic Exploitation

For the purposes of this assessment, the Test Team focused on Email and Web-based exploitation.

Social Engineering attacks involving e-mails are often referred to as phishing. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using e-mail or an instant message. Web Based Exploitation commonly follows E-Mail Exploitation in two common forms. In its first form, phishing e-mails attempt to lure users to a fictitious website wherein they are prompted to enter sensitive information. The information users enter on the website is being collected behind the scenes by an attacker who is logging all activity. In its second form, phishing e-mails prompt users to click on a malicious

link, modified to carry out exploitation of a user's system or a cross-site scripting (XSS) attack. These harvesting techniques are substantially less time consuming than trying to penetrate a system using purely technical resources. The techniques are often exploited as many organizations do not provide awareness training to their employees. In order for e-mails and websites to appear more legitimate, attackers will use the information they gathered through open source Internet research.

4.3 Penetration Testing Results

4.3.1 Direct Penetration Test

The Test Team identified nine State systems that were accessible from the internet to target during this phase of the test. Attacks against 8 of the systems were not successful as the targeted servers appeared to have been patched or otherwise not vulnerable. However, the test team was successful in creating a local account with administrator privileges on a system used by the University system for scheduling which now falls under the purview of ITD. It appears that none of the attacks were detected or reported by the State's intrusion detection monitoring processes.

The system that was successfully exploited did not have a password set on an Oracle Database related service. The test team was able to utilize this weakness to write a file on the server in the Start directory of the local Administrator account. When a legitimate systems admin logged in as Administrator, this file executed and added an account with Administrator privileges. The test team was not able to log into the account once it was created as the attack script used assigned a null password to the account. By default, Windows 2003 will not allow logins to accounts with null passwords. If the script had set a password on the account, the test team would have been able to get full command line access to the system. In a real world situation, once the attacker realized this, the attack would have been rerun to correct the password issue, and once the Administrator account was logged into again the system could be fully compromised. Due to test timing constraints, the scenario was ended without further exploitation. System administrators verified that the "ManTech" account was created on the system and deleted it.

4.3.2 Social Engineering

Scenario One

The test team created a fake Outlook Web Access (OWA) site, mirroring the State's official OWA login page, in an attempt to capture usernames/passwords. An email was then sent to nd.gov email addresses collected by utilizing the email search page on the main www.nd.gov website. The email appeared to come from the "ITD Help Desk" and requested users click on the link https://www.ndwebmail.gov to test out a new server that had been deployed. This link actually directed users to https://www.ndwebmail.com, which was the site set up and controlled by the test team. Any username/password entered into this site was captured by the test team.

Original attempts to spoof the sender of the email as "itd@nd.gov" were blocked at the States spam filter. The test team then modified the email to come from "itd@ndwebmail.com" to

bypass the filters and then sent a total of 110 emails to "@nd.gov" addresses. Out of these emails, the team was able to capture one valid username and password.

Within 3 hours of the first email being sent, one of the recipients notified the official ITD Service Desk about the phishing email. ITD Security was then notified by the State's Trusted Agent that the email was part of a test. ITD Security continued their normal course of action and blocked access to the malicious site and the IT Service Desk sent a notification email to all state email addresses notifying them of the fraudulent email and requested any users that entered their credentials to the site change their passwords.

Scenario Two
The test team created an email that would cause users' systems to visit a malicious website and would attempt to exploit users' systems through an Internet Explorer vulnerability. The email was sent from "memberservices@espn-sweepstakes.com" and directed users to visit http://www.espn-sweepstakes.com to enter to win an all expenses paid trip to see a professional football game.

This email was sent to 330 "@nd.gov" users over a two day period. All addresses were gathered by utilizing the email search page on the main www.nd.gov website. Over this period there were 7 different attempts to access the site from the State's network. These visits did not result in successful exploitation of any State systems as the systems are believed to have been patched. The email was not reported to ITD by any State users and it does not appear that the State's intrusion detection flagged the exploit attempts.

Although the exploit was unsuccessful in this case, this exercise shows the susceptibility of users to access malicious content on the internet. Had a more current public exploit or zero-day been available, these users' systems could have been compromised and used as a jumping point to the internal State network.

4.3.3 Vulnerability Findings

The Test Team targeted a total of nine systems for exploitation, and successfully exploited a single system. Although the Test Team could not fully access this system, given time the issues could have been corrected and the system fully exploited. The scope of the penetration test was limited, but an attacker operating without scope or time restrictions could easily expand access within the State's network. In addition, using social engineering techniques, the test team was successful in its attempts to gain account credentials and showed the susceptibility of users to access malicious content on the Internet.

5. APPLICATION SECURITY ASSESSMENT

5.1 Overview

Web-based applications are used extensively by many organizations to provide Internet users access to a variety of types of information. These applications are increasingly complex with numerous components such as databases which may contain sensitive data. Often custom developed applications focus on the functionality of the application and not the security of the application. An organization might have a secure web server, but if the web-based application that is hosted on the server can be compromised, then those protections are not effective. Application Security Assessments give organizations an opportunity to thoroughly and realistically evaluate the security posture of an application and its associated components.

During the period of August 22- September 5 2007, the Test Team performed an application security assessment of the State of North Dakota's PeopleSoft Financials Application. ConnectND is the name given to the PeopleSoft deployment within the State of North Dakota. PeopleSoft is a commercial suite of applications providing a wide range of management functions including financial, personnel, and project management.

5.2 Application Security Assessment Approach

ManTech SMA used automated and manual methods to test the security of the selected application. We used a two-tiered approach to application security testing. We began by using industry leading automated tools such as WebInspect and AppDetective to capture a high-level security snapshot of the application. We then took testing one step further by providing expert analysis of these results and probing further into the application with manual techniques and custom written tools that can help find more elusive and less well known security flaws.

Advanced tools and techniques were used to find flaws in the following categories:

- Un-validated input
- Non-functioning access controls
- Authentication and session management issues
- Cross-site scripting flaws
- Buffer overflows
- Injection flaws
- Improper error handling
- Insecure data storage
- Denial of service (DoS)

Based on the business logic of the application, the application is also tested using various roles. These roles correspond to differing levels of access to the system and the data it contains. This testing ensures that an account with one role (e.g. user) cannot access other portions of the application restricted to a different role (e.g. administrator functions). These tests are repeated for each role within the system, ensuring that access controls function properly at all levels.

5.3 Application Security Assessment Results

ManTech SMA performed a review of the State's PeopleSoft Financial application to access its overall security posture. This review included both manual and automated testing techniques.

5.3.1 General Recommendations

The following recommendations were provided to the State to improve the overall security of the application.

Ensure systems hosting application are kept up to date
All systems hosting components of the application should be maintained at the most current version and patch levels for both operating system and all applications installed on the system. A lapse in maintaining proper patch levels at any level of the system can compromise the overall security of the system.

Prevent simultaneous logins
Currently, simultaneous logins are permitted to the application. This allows multiple users to use a single username/password to access the application simultaneously. Users should be restricted to a single session at any given time.

5.3.2 Vulnerability Findings

Multiple tools were used to perform automated vulnerability and application scans against the systems comprising the application as requested by the State. A web proxy and other testing tools were also used to perform manual checks of the application.

Overall, there were 2 vulnerability findings with the application and its associated components; 1 high risk vulnerability dealing with the operating system installed on the application host and 1 low risk design flaw. The overall internal security mechanisms within the application are very strong and, with the exception of a possible operating system patching issue, the State has deployed the application in a secure manner.

6. SUMMARY

The findings presented in this report are typical of organizations with an enterprise the size of the State of North Dakota. Organizations with large numbers of systems face the challenge of maintaining a variety of operating systems, network devices, applications, and databases. Overall, the vast majority of vulnerabilities found during testing tended to be applications that were not kept current on patches. These results show a marked improvement over the assessment conducted in 2005.

The translation of public IP addresses to systems directly on the State's internal network is a concern. A compromise of just one of these servers would give direct access to the internal network to an external attacker. Once on the internal network, the attacker would encounter only limited restrictions to the State's most critical systems. Placing these publicly accessible servers into a DMZ configuration adds a crucial layer of protection to the internal network.

Due to the shared nature of the State's internal network (as with the external), the security posture of each agency directly impacts the security of the other participants. Poorly maintained and patched systems in one agency could lead to compromise of these systems and inevitably the use of these systems for attacks against other State systems across the internal network. While the State seems to be doing an excellent job ensuring Operating System patches are deployed, a weakness exists in ensuring applications installed on these systems are patched as well.

The number of systems directly connected to the Internet should be restricted to specific servers and services. This reduces the overall threat to the State as a smaller number of systems are available from the Internet. It also reduces the number of systems which require monitoring and allows administrators and security personnel to concentrate on securing a much smaller subset systems and vulnerabilities. In addition all systems should be maintained at the most current version and patch levels for both operating system and applications to decrease the State's exposure to vulnerabilities.

Another concern is that many systems allowed unrestricted access from the Internet. In some instances, applications (e.g. VPN, web servers, etc.) require access from any Internet user. However, IP-based access controls should be implemented for State Internet systems in the majority of circumstances to restrict access to these services to authorized systems when possible. Any services that should not be publicly accessible, such as NetBIOS, should be filtered.

Finally, the results of the penetration testing illustrate that users continue to be the weakest link to an organization's security posture. Attackers often only need to gain access to one system to provide a firm foothold from which to expand the exploitation of an organization. Continuing education and training of users is necessary to minimize the risk to an organization. This testing also enforces the importance of keeping systems patched in a timely manner and the importance of monitoring network and system activity for suspicious events.